Participación y despliegue de CTFs como herramienta para fortalecer la formación en ciberseguridad

Javier Díaz, Paula Venosa, Nicolás Macia, Einar Lanfranco, Alejandro Sabolansky, Mateo Durante, Damián Rubio, Jeremías Pretto
Laboratorio de Investigación de Nuevas Tecnologías Informáticas (LINTI).
Facultad de Informática. Universidad Nacional de La Plata
50 y 120 La Plata
{jdiaz, pvenosa, nmacia, einar, asabolansky, mdurante, drubio, jpretto}@linti.unlp.edu.ar

RESUMEN

A través de diferentes proyectos y con un grupo de investigación que se encuentra en continuo crecimiento, el Laboratorio en Nuevas Tecnologías Informáticas (LINTI) desarrolla de manera ininterrumpida desde el año 2000 una línea de investigación en ciberseguridad [1][2]. Entre los hitos más destacados se encuentran la puesta en marcha de la autoridad de certificación UNLP PKIGRID [3] en el año 2007 la cual fue acreditada por TAGPMA [4] y que actualmente forma parte del repositorio de autoridades de certificación académicas confiables TACAR [5][6], así como la creación del primer CSIRT académico de la Argentina CERTUNLP [7]. Años más tarde, los docentes e investigadores del área comenzaron a participar más activamente en competencias de tipo CTF[1].
En el presente trabajo se describen los CTFs, la experiencia y logros del equipo, la implicancia de su aplicación en lo que hace a la metodología de enseñanza, su aplicación en materias de grado relacionadas a la temática así como en lo que hace a formación de recursos humanos en seguridad, y en particular a la colaboración en la formación de equipos de respuesta de incidentes, comenzando por la comunidad académica local y generando sinergias a partir de la coordinación de actividades en grupos de trabajo regionales e internacionales.

Palabras clave: Ciberseguridad, seguridad inteligente, CTFs, Seguridad en aplicaciones, IoT

CONTEXTO

La línea de investigación en ciberseguridad que incluye la “Participación y despliegue de CTFs como herramienta para fortalecer la formación en ciberseguridad” presentada en este trabajo, se inserta en el proyecto de investigación "Internet del Futuro: Ciudades Digitales Inclusivas, Innovadoras y Sustentables, IoT, Ciberseguridad, Espacios de Aprendizaje del Futuro" [8] del Programa Nacional de Incentivos a docentes investigadores, que se desarrolla en el LINTI de la Facultad de Informática de la Universidad Nacional de La Plata (UNLP). Este proyecto está acreditado por la UNLP y financiado por partidas del presupuesto nacional.

1. INTRODUCCIÓN

Los CTFs (Captura de bandera o Capture The Flag por su sigla en inglés) son competencias de

[1] CTF: Capture the flag

seguridad informática que posibilitan el aprendizaje de distintas cuestiones vinculadas con la ciberseguridad de manera lúdica. El objetivo de las competencias es descubrir "flags". Las llamadas "flags" (banderas) son piezas de información que se ocultan, ya sea en servidores solo accesibles a través de algún protocolo o en una aplicación vulnerable, cifrándolas en un archivo o colocándolas no disponibles a simple vista. Durante el tiempo que dura la competencia, se liberan distintos desafíos en donde los equipos participantes aplican diferentes técnicas entre las que se encuentran la ingeniería inversa, hacking, criptoanálisis, ingeniería social para hacerse con las flags.

Este tipo de competencias suelen ser de dos modalidades: (i) los CTFs del tipo *jeopardy* cuentan con desafíos que al resolverlos entregan un texto secreto que se denomina bandera o *flag*. Este *flag* no es más que un texto bajo un formato específico, y el descubrirlo implica la resolución del desafío y (ii) los CTFs de ataque-defensa, donde cada equipo debe defender un servidor o una red con servicios vulnerables del resto de los participantes. Cada equipo tiene tiempo para arreglar los problemas en sus servicios evitando ser atacados y desarrollar tools para aprovechar vulnerabilidades presentes en la red del resto de los equipos. Los puntos se obtienen al proteger los servicios propios (puntos de defensa) y al atacar exitosamente a los servicios de los otros equipos (puntos de ataque) [9][10].

Muchos de los desafíos o retos están directamente relacionados con problemas de seguridad actuales o contemporáneos al momento en que se desarrolla la competencia y los patrones de resolución de problemas son similares a los que se aplican en la vida real. El hecho de resolverlos actúa, en muchos casos, como disparador para encontrar nuevos problemas en el ámbito laboral donde los miembros del equipo se desempeñan.

Tras la culminación de las competencias, es habitual que quienes resuelven retos, publiquen las resoluciones de los mismos [11]. Esta práctica sirve como fuente de aprendizaje para quien consulte dichas resoluciones. Para los que hayan llegado a resolver el ejercicio, sirve para aprender sobre posibles alternativas de resolución. Para aquellos que no hayan logrado resolver el ejercicio, sirve para aprender algo nuevo o para medir qué tan cerca se estuvo de alcanzar la solución con su análisis e intentos previos.

Para que un CSIRT preste sus servicios y crezca, resulta fundamental el desarrollo de habilidades específicas relacionadas con la ciberseguridad como ser el testeo de la seguridad de un sistema o la corrección del sistema para que no sea vulnerable. Investigar sobre nuevas vulnerabilidades, conocer técnicas y herramientas para detectar dichas vulnerabilidades, como así también estándares adecuados para llevar a cabo el proceso de testeo de seguridad, son tareas que forman parte del desafío de contar con sistemas cada vez más seguros en las organizaciones.

Tanto la participación en eventos del tipo CTF como la lectura de las resoluciones (o writeups) favorecen el desarrollo de habilidades relacionadas con la seguridad de sistemas, redes, comunicaciones y servicios. Esto representa un método alternativo de capacitación y actualización contínua para los distintos recursos humanos que forman parte del grupo de investigación.

La participación en este tipo de competencias suele ser en equipo. Esto fomenta el espíritu de compartir conocimientos y experiencias, como

así también el de relacionarse con personas interesadas en las mismas temáticas.

Los CTFs pueden utilizarse como herramienta para entender la ciberseguridad a partir de una actividad lúdica. La aplicación de la gamificación como una metodología de enseñanza alternativa se aplica en varios países del mundo. Las competencias de tipo CTF se consideran una forma de llevar a cabo esta metodología [12][13].

2. LÍNEAS DE INVESTIGACIÓN, DESARROLLO E INNOVACIÓN

En la actualidad, como se ha mencionado, la línea de trabajo de formación y actualización a través del desarrollo de competencias mediante la continua participación en concursos de tipo CTF, aquí presentada, constituye uno de los ejes fundamentales del grupo de investigación en ciberseguridad.

Además de ello, el grupo continúa investigando y trabajando en las siguientes actividades:

- Gestión de incidentes de seguridad.
- Monitoreo de seguridad inteligente.
- Detección y análisis de vulnerabilidades en distintos tipos de dispositivos, protocolos y tecnologías.
- Gestión de seguridad informática en infraestructuras de red y servicios.
- Forensia digital.
- Infraestructura de clave pública PKI.
- Desarrollo seguro de software.

3. RESULTADOS OBTENIDOS Y ESPERADOS

Como principales objetivos se plantean algunos generales como:

- Consolidar la línea de investigación en ciberseguridad y su aplicación en la docencia y la extensión, trabajando sobre los temas emergentes asociados a las metodologías y paradigmas que surgen día a día.
- Transmitir la experiencia adquirida en distintos proyectos y actividades a los alumnos de las cátedras de grado y postgrado con contenidos afines de nuestra Facultad.

Y otros más específicos como:

- Consolidar el equipo de CTF de la UNLP (llamado CERTUNLP o SYPER)
- Mejorar los resultados de años anteriores, tanto en conferencias como en el ranking mundial mantenido por CTFtime.
- Organizar nuevos eventos a nivel nacional y regional.

Entre los resultados que se han obtenido en este último tiempo:

- En marzo de 2020 se organizó una competencia de ciberseguridad utilizando una metodología basada en CTFs en el marco del evento de Metared denominado “Jornada de Ciberseguridad para Universidades 2020”.
- En el año 2018 y en el año 2019, el grupo obtuvo el primer puesto en el CTF organizado por Ekoparty, la conferencia de Seguridad más importante de la región. Desde el año 2017, el equipo ocupa el 1er puesto de Argentina en el ranking mantenido por CTFtime [14] [15].
- Mejora contínua de los servicios prestados por CERTUNLP a la comunidad

académica, aplicando conceptos aprendidos a partir de la participación en CTFs.

- Aplicación de la metodología de enseñanza utilizando competencias de tipo CTF en las siguientes materias de grado: Introducción a la Ciberseguridad, Desarrollo Seguro de Aplicaciones, Introducción a la Forensia Digital y Seguridad y Privacidad en Redes.
- Formación de un equipo interclaustro, compuesto por docentes y alumnos, que participan en competencias de tipo CTF y que se reúnen periódicamente para intercambiar conocimientos adquiridos en distintas temáticas de interés. El equipo se constituyó a partir de la convocatoria realizada por este grupo en el año 2017, invitando a todos los alumnos y docentes interesados a participar.
- Definición de un circuito para el desarrollo de nuevos retos, así como también la infraestructura a utilizar para su instalación y mantenimiento. Esto fue desarrollado en de manera conjunta entre distintos docentes parte del grupo de investigación, de modo que las distintas cátedras involucradas en temáticas de ciberseguridad, utilicen las mismas soluciones para la implementación de sus CTFs.
- Tanto en las cátedras de grado como en las "Jornada de Ciberseguridad para Universidades 2020" se utilizó la plataforma Open Source CTFd [16]. La misma, ha sido desplegada y configurada en servidores del LINTI.

4. FORMACIÓN DE RECURSOS HUMANOS

En esta línea de investigación trabaja un grupo de docentes/investigadores del LINTI (Laboratorio de Investigación en Nuevas Tecnologías Informáticas) de la Facultad de Informática de la UNLP (Universidad Nacional de La Plata). Este equipo de trabajo también forma parte de CERTUNLP, el CSIRT Académico de la Universidad Nacional de La Plata, ámbito en el que se aplican las distintas temáticas incorporadas utilizando las competencias de tipo CTF.

En el último año, se realizaron dos tesinas de grado, dirigidas por los profesores Einar Lanfranco y Paula Venosa, autores de este trabajo.

La primera de las tesinas, denominada "Automatizando la resolución de problemas en competencias de seguridad informática" de los alumnos Jeremías Pretto y Facundo Basso, profundizó la investigación y el desarrollo de herramientas que pueden ser utilizadas en competencias tipo CTF. Como resultado de este trabajo se realizaron dos herramientas para resolver retos de los que se presentan habitualmente. La primera es para ayudar a los participantes novatos a acercarse a la solución de problemas y la segunda para enfrentar los retos que involucran distintos tipos de ataques a RSA.

La segunda tesina titulada "'Capture the flag' aplicada a la enseñanza de ciberseguridad en escuelas secundarias" fue realizada por los alumnos Patricio Bolino y Gabriela Suárez y tuvo como objetivo organizar CTFs para alumnos de escuelas secundarias, adecuando contenidos y retos para sortear barreras que dificultan la participación de los adolescentes sin ningún tipo de conocimientos previos.

5. REFERENCIAS

[1] - Díaz, Francisco Javier, Molinari, Lía Hebe, Venosa, Paula, Macia, Nicolás, Lanfranco, Einar Felipe, Sabolansky, Alejandro Javier (2018). "Investigación en ciberseguridad: un enfoque integrado para la formación de recursos de alto grado de especialización". WICC 2018 (Workshop de Investigadores en Ciencias de la Computación). UNNE, Corrientes, Argentina. Abril de 2018. Libro de Actas XX Workshop de Investigadores en Ciencias de la Computación. ISBN 978-987-3619-27-4.

[2] Díaz, Francisco Javier, Molinari, Lía Hebe, Venosa, Paula, Macia, Nicolás, Lanfranco, Einar Felipe, Sabolansky, Alejandro Javier (2019). "Investigación en ciberseguridad: nuevos desafíos para adaptarse a nuevos paradigmas". WICC 2019 (WICC 2019, Universidad Nacional de San Juan). Libro de Actas XXI Workshop de Investigadores en Ciencias de la Computación.pp 905-910. ISBN 78-987-3984-85-3

[3] PKIGrid: http://www.pkigrid.unlp.edu.ar/

[4] TAGPMA: The Americas Grid Policy Management Authority http://www.tagpma.org/

[5] TACAR: Trusted Academic Certification Authority Repository https://www.tacar.org/

[6] Clave de la UNLP PKIGrid en TACAR: https://www.tacar.org/cert/install/7

[7] CERTUNLP: CSIRT académico de UNLP https://cespi.unlp.edu.ar/cert

[8] Proyecto: F020 - Internet del Futuro. Ciudades Digitales, Inclusivas, Innovadoras y Sustentables, IoT, Ciberseguridad, Espacios de aprendizaje del Futuro. https://cyt.proyectos.unlp.edu.ar/projects/11-f020

[9] "CTF: Learn Hacking by Playing" (14 de agosto de 2019). https://www.sothis.tech/en/ctf-learn-hacking-by-playing/

[10] "CTF: Entrenamiento en seguridad informática" (26 de febrero de 2014). https://www.incibe-cert.es/blog/ctf-entrenamiento-seguridad-informatica

[11] Writeups de CTFtime. https://ctftime.org/writeups

[12] Mc Daniel Lucas, Talvi Erik, Hay Brian, "Capture the Flag as Cyber Security Introduction" en IEEE Computer Society Washington, "Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS)", University of Alaska Fairbanks, 2016.

[13] Cheung Ronald S., Cohen Joseph P., Lo Henry Z., Elia Fabio, "Challenge Based Learning in Cybersecurity Education", Department of Computer Science, University of Massachusetts, Boston, MA, USA, 2011.

[14] SYPER https://ctftime.org/team/2003

[15] Clasificación de SYPER en Argentina: https://ctftime.org/stats/2017/AR

[16] CTFd https://github.com/CTFd/CTFd